Doc Code: AP.PRE.REQ .

PRE-APPEAL BRIEF REQUEST FOR REVIEW

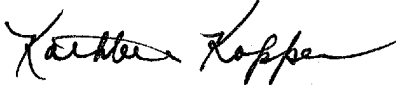|	
PRE-APPEAL BRIEF REQUEST FOR REVIEW	Docket Number (Optional): **4015-721/P12472-US1**

I hereby certify that this correspondence is being deposited with the United States Postal Service electronically.

Date: **August 11, 2006**

Signature: *Kathleen Koppen*

Typed or printed name: **KATHLEEN KOPPEN**

Application Number: **09/727,062**	Filed: **November 30, 2000**
First Named Inventor: **Dent**	

Art Unit: **2134**	Examiner: **PIOTR POLTORAK**

Applicant requests review of the final rejection in the above-identified application. No amendments are being filed with this request

This request is being filed with a notice of appeal and time extension request.

The review is requested for the reason(s) stated on the attached sheet(s).
Note: No more than five (5) pages may be provided.

I am the

☐   applicant/inventor
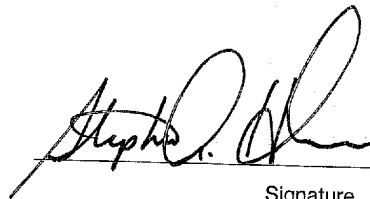
☐   assignee of record of the entire interest.
See 37 CFR 3.71. Statement under 37 CFR 3.73(b) is enclosed.
(Form PTO/SB/96)

☒   attorney or agent of record
Registration Number:_____47,642_____

☐   attorney or agent acting under 37 CFR 1.34.
Registration Number if acting under 37 CFR 1.34_____

_____
Signature

_____Stephen A. Herrera_____
Typed or Printed Name

_____(919) 854-1844_____
Telephone Number

_____August 11, 2006_____
Date

NOTE: Signatures of all the inventors or assignees of record of the entire interest or their representative(s) are required. Submit multiple forms if more than one signature is required, see below*.

☐   *Total of _____ form(s) is/are submitted.

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of
Dent

Serial No.: **09/727,062**

Filed: **November 30, 2000**

For: **ANTI-SPOOFING PASSWORD PROTECTION**

Docket No: **4015-721**

)
)
)
)
)
)
)
)
)
)
)
)
)
)

PATENT PENDING

Examiner: Piotr Poltorak

Group Art Unit: 2134

Confirmation No.:2720
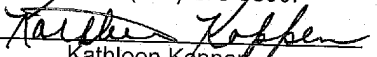
Mail Stop AF
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Applicants submit the following remarks in support of the Pre-Appeal Brief Request for Review attached herewith. Claims 1-5, 7-12, 14-15, 17-18, and 20 are currently pending with claims 1 and 11 being independent. The Examiner finally rejected claims 1 and 11 as being obvious over Windows NT as evidenced by the "Windows NT Server 4 Security Handbook" to Hadfield and the "NT Workstation Resource Kit" (http://web.archive.org/web/20000831044112/is-it-true.org/nt/atips/atips71.shtml), in view of Foster (U.S. Pat. No. 5,652,890).

The present invention employs authentication indicia that functions as a "reverse password" that is used by a computer to authenticate valid password entry screens. The presence or absence of the authentication data indicates to the user whether the password entry screen is valid. Because the authentication data is stored in a secure memory, it is not

possible for a rogue program to spoof the password entry screen. Additional measures can be taken to inhibit execution of application programs, such as a video capture program, while the password entry screen is displayed.

Simply stated, the Examiner has ignored the functional language of the claims that describes the function of the claimed authentication indicia. Claim 1 recites, *inter alia*, authentication indicia that is used "for authenticating password entry screens to a user." For the convenience of the Panel, claim 1 appears below in its entirety.

> 1. A method implemented by a security module in a computing device of performing a password-protected secure function, said method comprising:
> storing authentication indicia for authenticating password entry screens to a user in a memory of the computing device;
> receiving a command to execute a password-protected secure function;
> temporarily halting execution of programs not needed by the security module while the data entry screen is displayed;
> prompting the user to enter a password associated with the secure function by displaying a password entry screen containing the authentication indicia responsive to receiving the command;
> removing the data entry screen from the display;
> restarting halted programs after the password entry screen is removed from the display; and
> executing the password-protected secure function based on the validity of the password entered by the user.

The authentication function of claim 1 is performed by including the authentication indicia on the password entry screen when the password entry screen is displayed. The user can differentiate a valid password entry screen from an invalid or "spoofed" password entry screen by the presence of the authentication indicia. A valid password entry screen would always contain the authentication indicia while an invalid password entry screen would not.

The Examiner equates the claimed authentication indicia to a user name on a Windows NT password entry screen. Specifically, the Examiner contends that the presence or absence of the user name authenticates the Windows NT password entry screen as valid or invalid to the user. This contention is wholly incorrect and completely unsupported by the cited art. The user name on an NT password entry screen is used only to authenticate the user to the computer.

It's presence or absence does nothing to authenticate that screen as valid to the user. User names are not secure, and therefore, are just as prone to being spoofed as the password entry screen itself. A user has no way of knowing whether a conventional NT password entry screen is valid or invalid based on the presence or absence of a mere user name. Any assertion to the contrary is mere conjecture.

Indeed, the Examiner does not support this contention with any citation to the intrinsic record. Rather, the Examiner simply advances the naked assertion that a user expects to see the user name on a password entry screen, and therefore, its absence "would alert the user that the displayed password entry screen MAY NOT BE AUTHENTIC." *Advisory Action*, p. 2, ¶14 (emphasis in original). The references do not even hint that the absence of a user name on a password entry screen would alert the user as the Examiner contends. The Examiner has simply invented a new functionality for the user name disclosed by the prior art, and then used that new functionality as reason to reject the claims. This sort of unsubstantiated reasoning, however, is exactly the type of *legally improper* reasoning routinely rejected by both the Board and the Federal Circuit.

None of the references, alone or in combination, teaches or suggests storing authentication indicia in a memory for authenticating password entry screens, or displaying password entry screens containing the authentication indicia. The user name entered by the user to gain access to a computer authenticates the user to the computer. It is not authentication indicia for authenticating password entry screens to the user, nor would anyone skilled in the art ever believe a user name to perform that function. Accordingly, the §103 rejections of claim 1 fails as a matter of law.

Additionally, the §103 rejection of claim 1 also fails because the references do not teach or suggest, alone or in combination, <u>temporarily halting execution of programs</u> not needed by the security module <u>while the password entry screen is displayed</u>, and <u>restarting the halted</u>

programs after the password entry screen is removed from the display. The Examiner admits

that neither of the NT-based references teaches or suggests this aspect, but asserts that Foster

does. This assertion is also incorrect and unsupported by the cited references.

Foster discloses generating an interrupt to force a microprocessor in a laptop computer

to switch in and out of a protected mode. Foster explicitly discloses when such an interrupt

would be generated. Column 3, lines 31-36 (the same passage cited by the Examiner to

support the rejection), discloses that a user might wish to leave his system without exiting any

running applications or turning the system off. However, the user would still want to prevent

others from accessing the computer. Whatever interrupts Foster does or does not generate at

this point is irrelevant. The user in Foster is already logged onto the system at the time the

interrupt is generated. Indeed, were the user not already logged on and authenticated to the

system, the user would not have to prevent others from accessing or viewing currently

executing applications.

Foster does not teach or suggest temporarily halting execution of programs not needed

by the security module while the password entry screen is displayed, and restarting the halted

programs after the password entry screen is removed from the display. Neither do the other

references as admitted to by the Examiner. Therefore, the §103 rejection of claim 1 fails and its
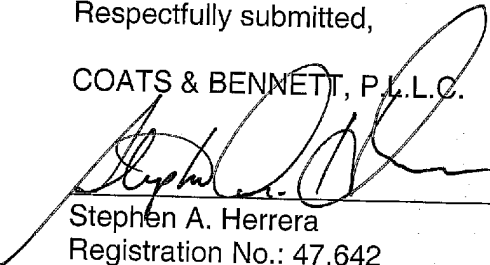
dependent claims fail and must be withdrawn.

The Examiner also rejected claim 11 under §103 over the same references and for

substantially the same reasons as those cited for claim 1. Claim 11, however, also recites that

the authentication indicia that is used "for authenticating password entry screens to a user," and

that a secure processor temporarily halts execution of programs not needed by the security

processor while the password entry screen is displayed, and restarts the halted programs after

the password entry screen is removed from the display. Accordingly, for reasons similar to

those stated above, the §103 rejection of claim 11 and its dependent claims fail and must be withdrawn.

For the foregoing reasons, the cited references do not teach or suggest, alone or in combination, independent claims 1 or 11. Therefore, the §103 rejections of independent claims 1 and 11, and of their respective dependent claims, fail as a matter of law and must be withdrawn. Accordingly, Applicant respectfully requests that the Panel overturn all rejections and allow all pending claims.

Respectfully submitted,

COATS & BENNETT, P.L.L.C.

Dated: August 11, 2006

Stephen A. Herrera
Registration No.: 47,642

P.O. Box 5
Raleigh, NC 27602
Telephone: (919) 854-1844
Facsimile: (919) 854-2084